

# Technical Cybersecurity

Bulb Attack!

# Attack Process

## RECON

---

- ▶ What versions of software?
- ▶ Known flaws?
- ▶ Can I access the vector?
- ▶ Default credentials?
- ▶ Easy credentials?
- ▶ What kind of traffic?
- ▶ Is the vector vulnerable?
- ▶ Is the vector exploitable?

## ***Attack Surface***

**Vector 0:** Bluetooth

**Vector 1:** HTTP Server

**Vector 2:** SSH Server

**Vector 3:** Misc Ports

**Vector 4:** DNS

**Vector 5:** HTTP Traffic

**Vector 6:** TCP/IP Traffic

**Vector 7:** Power Interface

**Vector 8:** Updates

# Attack Process

## WHAT CAN WE DO?

---

- ▶ We've checked out the system and we know what's there
- ▶ We have researched existing vulnerabilities and know if they're exploitable
- ▶ We have an idea how to exploit those
- ▶ Develop that idea into methods we can use to exploit

## ***Attack Surface***

**Vector 0:** Bluetooth

**Vector 1:** HTTP Server

**Vector 2:** SSH Server

**Vector 3:** Misc Ports

**Vector 4:** DNS

**Vector 5:** HTTP Traffic

**Vector 6:** TCP/IP Traffic

**Vector 7:** Power Interface

**Vector 8:** Updates

# Attack Process

## TRIGGER!

---

- ▶ Use the method to attack the actual device
- ▶ We want to get onto the device and then establish *persistence* (although not always needed)
- ▶ Trigger the exploit and install our code (or use the code that already exists)

## ***Attack Surface***

**Vector 0:** Bluetooth

**Vector 1:** HTTP Server

**Vector 2:** SSH Server

**Vector 3:** Misc Ports

**Vector 4:** DNS

**Vector 5:** HTTP Traffic

**Vector 6:** TCP/IP Traffic

**Vector 7:** Power Interface

**Vector 8:** Updates

# Attack Process

## DO OUR THING

---

- ▶ So we now have some control over the device, we want to establish communication for Command & Control (C2)
- ▶ Escalate if needed

Repeat to further  
penetrate

## ***Attack Surface***

**Vector 0:** Bluetooth

**Vector 1:** HTTP Server

**Vector 2:** SSH Server

**Vector 3:** Misc Ports

**Vector 4:** DNS

**Vector 5:** HTTP Traffic

**Vector 6:** TCP/IP Traffic

**Vector 7:** Power Interface

**Vector 8:** Updates

Okay, but what does this  
have to do with  
defending systems?